UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/804,489	03/18/2004	Vincent J. Zimmer	42P18506	7634

7590 12/01/2006

Anthony H. Azure
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
VO, TED T	

ART UNIT	PAPER NUMBER
2191	

DATE MAILED: 12/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/804,489	ZIMMER ET AL.	
	Examiner	Art Unit	
	Ted T. Vo	2191	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 3/18/04.

Claims 1-23 are pending in the application.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. The claims 12-18 are rejected under 35 U.S.C 101 because the claimed invention is directed to non-statutory subject matter.

A claimed invention as a whole must accomplish a practical application. That is, it must produce a **"useful, concrete and tangible result"** State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. Media which are wireless, forms of energy, signals are not concrete and tangible.

As per Claims 12-18: Claims 12-18 claim an article of manufacture comprising a machine-accessible medium, where in the specification it includes

> a machine-accessible medium can include propagated signals such as electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.)

Claims 12-18 fails to meet the statutory claims under 35 U.S.C 101.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claims 1-23 are rejected under 35 U.S.C. 102(a) as being anticipated by Garfinkel et al., "Terra: A Virtual Machine-Based Platform for Trusted Computing", ACM, 2003.

Given the broadest reasonable interpretation of followed claims in light of the specification.

As per Claim 1: Garfinkel discloses,

A method, comprising: loading a virtual machine monitor (VMM) to support a plurality of virtual machines in a computer system, the VMM including a VMM multiplexer (see p.194, left col., last paragraph, "allow many virtual machines (VMs) to run...": *plurality of virtual machines.* See Figure 1, TVMM: "VMM": i.e., TVMM is loaded in a hardware platform)*; loading a first and a second virtual machine (VM) supported by the VMM* (p.194, left col., last paragraph; p. 196, left col., third paragraph);

and sharing a trusted hardware device between the first VM and the second VM using the VMM multiplexer (refer TVMM, T: trusted; see p. 194, right col., last paragraph, "multiplex").

As per Claim 2: Garfinkel discloses, *The method of claim 1 wherein the VMM is loaded from firmware, the firmware including instructions compliant with an Extensible Firmware Interface (EFI) specification* (See sec. 2.2, p.195-196, and p. 199, e.g., "firmware", "VM firmware", and see p.195, left col. Extensibility).

As per Claim 3: Garfinkel discloses, *The method of claim 1 wherein sharing the trusted hardware device comprises multiplexing a first request from the first VM and a second request from the second VM to the trusted hardware device using the VMM multiplexer* (See p. 194, right col., last paragraph, "multiplex", also see Figure 1).

As per Claim 4: Garfinkel discloses, *The method of claim 1, further comprising determining a first VM platform configuration and a second VM platform configuration* (See p. 194, right col., last paragraph, "configuring how...").

As per Claim 5: Garfinkel discloses, *The method of claim 4, further comprising: determining a compound platform configuration based on a combination of the first VM platform configuration and the second VM platform configuration; and storing the compound platform configuration in the trusted hardware device* (See Figure 1, interface section between TVMM and hardware platform, the and see sec. 4.4, start at p. 199).

As per Claim 6: Garfinkel discloses, *The method of claim 5 wherein the first VM platform configuration includes a first hash value based on information measured from the first VM and the second VM platform configuration includes a second hash value based on information measured from the second VM* (See p. 196, right col., all paragraphs, "VM's hash", the verifications of 1, 2, 3, etc.).

As per Claim 7: Garfinkel discloses, *The method of claim 5, further comprising sealing secret information from the first VM with the compound platform configuration using the trusted hardware device* (Refer to Terra's signatures such as seal storage in Figure 1, and see p. 195, left col., full sec. 2.1, "trusted platform", and see whole sec. 4.5, Device Driver Security).

As per Claim 8: Garfinkel discloses, *The method of claim 7, further comprising unsealing the secret information using the trusted hardware device if a current first VM platform configuration matches the first VM platform configuration* (See p. 195, left col., full sec. 2.1, "trusted platform", and see whole sec. 4.5, Device Driver Security).

As per Claim 9: Garfinkel discloses, *The method of claim 1, further comprising maintaining a queue of trusted hardware device requests by the VMM multiplexer, the trusted hardware requests sent to the trusted hardware device from the first VM and the second VM* (the operation of Figure 1).

As per Claim 10: Garfinkel discloses, *The method of claim 9, further comprising reporting a first request from the first VM is in progress when the trusted hardware device is polled by the first VM regarding the status of the first request, the first request actually waiting in the queue to be processed by the trusted hardware device* (the operation of Figure 1).

As per Claim 11: Garfinkel discloses, *The method of claim 1 wherein the trusted hardware device includes a trusted platform module (TPM)* (Figure 1, with sealed storage device).

As per Claim 12: Garfinkel discloses claim 12. See the rationale addressed in Claim 1.

As per Claim 13: Garfinkel discloses, *The article of manufacture of claim 12 wherein execution of the plurality of instructions further perform operations comprising: receiving a first VM platform configuration from the first VM, the first VM platform configuration including information measured from the first VM; computing a first virtual hash value based on the first VM platform configuration; receiving a second VM platform configuration from the second VM, the second VM platform configuration including information measured from the second VM; and computing a second virtual hash value based on the second VM platform configuration* (See p. 196, right col., all paragraphs, "VM's hash", the verifications of 1, 2, 3, etc., and see sec. 4.4 start at p, 199).

As per Claim 14: Garfinkel discloses, *The article of manufacture of claim 13 wherein execution of the plurality of instructions further perform operations comprising sending the first virtual hash value and the second virtual hash value to the TPM, the TPM to compute a compound hash value based on the first virtual hash value and the second virtual hash value* (See p. 196, right col., all paragraphs, "VM's hash").

As per Claim 15: Garfinkel discloses, *The article of manufacture of claim 14 wherein execution of the plurality of instructions further perform operations comprising sending a seal command to the TPM to seal secret information from the first VM with the compound hash value* (The operation of Figure 1, sealed storage device, see p. 196, right col., all paragraphs, "VM's hash").

As per Claim 16: Garfinkel discloses, *The article of manufacture of claim 15 wherein execution of the plurality of instructions further perform operations comprising sending an unseal command to the TPM from the first VM to unseal secret information associated with the first VM* (The operation of Figure 1, sealed storage device, see p. 196, right col., all paragraphs, "VM's hash").

As per Claim 17: Garfinkel discloses, *The article of manufacture of claim 12 wherein execution of the plurality of instructions further perform operations comprising maintaining a TPM request queue to queue a first TPM request from the first VM and a second TPM request from the second VM.* (The operation of Figure 1).

As per Claim 18: Garfinkel discloses, *The article of manufacture of claim 17 wherein execution of the plurality of instructions further perform operations comprising reporting the second TPM request is in progress if the TPM is polled by the second VM, the second TPM request actually waiting in the TPM request queue* (the operation of Figure 1).

As per Claim 19: Garfinkel discloses claim 19, see rationale addressed in Claim 1.

As per Claim 20: Garfinkel discloses claim 20,

The computer system of claim 19 wherein execution of the plurality of firmware instructions further perform operations comprising: maintaining a first VM platform configuration and a second VM platform configuration by the VMM multiplexer; and storing a compound platform configuration based on a combination of the first VM platform configuration and the second VM platform configuration in the trusted hardware device. See rational in the rejection of Claim 5.

As per Claim 21: Garfinkel discloses, *The computer system of claim 19 wherein execution of the plurality of firmware instructions further perform operations comprising maintaining a queue of trusted hardware device requests by the VMM multiplexer, the trusted hardware device requests sent to the trusted hardware device from the first VM and the second VM.* See rational in the rejection of Claim 9.

As per Claim 22: Garfinkel discloses claim 22, see rationale addressed in Claim 1. *The computer system of claim 19 wherein the firmware instructions compliant with an Extensible Firmware Interface (EFI) specification* (see p.195, left col. Extensibility).

As per Claim 23: Garfinkel discloses claim 23, see rationale addressed in Claim 11.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ted T. Vo whose telephone number is (571) 272-3706. The examiner can normally be reached on 8:00AM to 4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wei Y. Zhen can be reached on (571) 272-3708.

The facsimile number for the organization where this application or proceeding is assigned is the Central Facsimile number **571-273-8300**.

Any inquiry of a general nature or relating to the status of this application should be directed to the TC 2100 Group receptionist: 571-272-2100. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TTV
November 24, 2006

TED VO
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100